



Bank Spółdzielczy w Przecławiu

**REJESTRACJA UŻYTKOWNIKA PRZY UŻYCIU HASŁA
MASKOWALNEGO**

**SPAROWANIE URZĄDZENIA MOBILNEGO
Z BANKOWOŚCIĄ ELEKTRONICZNĄ**

OBSŁUGA APLIKACJI ASSECO MAA

Spis treści

PIERWSZE Logowanie do systemu	3
KOLEJNE LOGOWANIA.....	4
Obsługa tokena Asseco MAA na urządzeniu mobilnym	5
Powiązanie urządzenia mobilnego z bankowością elektroniczną	5
REALIZACJA PRZELEWU	10

KROK 1

PIERWSZE Logowanie do systemu

Po uruchomieniu systemu CUI <https://cbp.cui.pl> wyświetlane jest okno logowanie użytkownika.

- Aby zalogować się do systemu należy w polu Numer Identyfikacyjny wprowadzić **identyfikator użytkownika (PC.....)** i użyć przycisku [DALEJ].

The screenshot shows a light blue header with the word "LOGOWANIE" on the left and "PL" with a dropdown arrow on the right. Below the header is a white form area. At the top of the form is the label "Numer Identyfikacyjny" followed by a text input field containing the placeholder "Wpisz numer". Below the input field is a blue button labeled "DALEJ". Underneath the button is a lock icon and the text "Pamiętaj o podstawowych zasadach bezpieczeństwa." followed by a list of three security rules: 1. The login page address must start with https. 2. A lock icon must be visible in the address bar or status bar. 3. The certificate is issued by Asseco Poland S.A. through DigiCert Inc. Below the list is the text "Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem." and a link "Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)".

- Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia kodu dostępu - hasła pierwszego logowania z **wiadomości SMS lub otrzymane z Banku** .

The screenshot shows a light blue header with a back arrow on the left and the word "LOGOWANIE" on the right. Below the header is a white form area. At the top of the form is the label "Kod dostępu" followed by a row of 24 empty input boxes, each numbered from 1 to 24. Below the input boxes is a blue button labeled "ZALOGUJ".

- Następnie system poprosi o ustawienie **własnego hasła** (kod dostępu)– należy podać najmniej 10 znaków i maksymalnie 24 i nie powinien zaczynać się od cyfry 0.

The screenshot shows a light blue header with a back arrow on the left and the text "NADAWANIE NOWEGO KODU DOSTĘPU" on the right. Below the header is a white form area. At the top of the form is a lock icon and the text "Polityka bezpieczeństwa banku wymaga zmiany hasła." Below this is the label "Identyfikator użytkownika" followed by a masked input field. Below that is the label "Nowy kod dostępu" followed by a text input field with the placeholder "Wpisz kod dostępu". Below that is the label "Powtórz nowy kod dostępu" followed by a text input field with the placeholder "Wpisz ponownie nowy kod dostępu". At the bottom of the form is a blue button labeled "ZAPISZ I ZALOGUJ".

Użytkownik zostaje zalogowany.

KOLEJNE LOGOWANIA

- Przy kolejnych logowaniach należy wpisać wybrane znaki z hasła (hasło maskowalne) – w polu Kod dostępu, pozostałe znaki z hasła są ukryte i zastąpione znakiem „•”. Po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

← LOGOWANIE

Kod dostępu

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

ZALOGUJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę Thawte lub DOMENY.PL

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po wprowadzeniu (w polu Kod dostępu) poprawnego kodu uwierzytelniającego należy użyć przycisku [ZALOGUJ]. System weryfikuje wprowadzone dane i jeżeli stwierdzi ich poprawność użytkownik zostanie zalogowany.

KROK 2

Obsługa tokena Asseco MAA na urządzeniu mobilnym

- Instalacja aplikacji mToken Asseco MAA na urządzeniu mobilnym.
TELEFON MUSI POSIADAĆ BLOKADĘ EKРАНU, BEZ BLOKADY APLIKACJA NIE DZIAŁA.

W sklepie: Google Play lub App Store należy wpisać nazwę **mToken Asseco MAA** i kliknąć **POBIERZ**



Android 6.x i

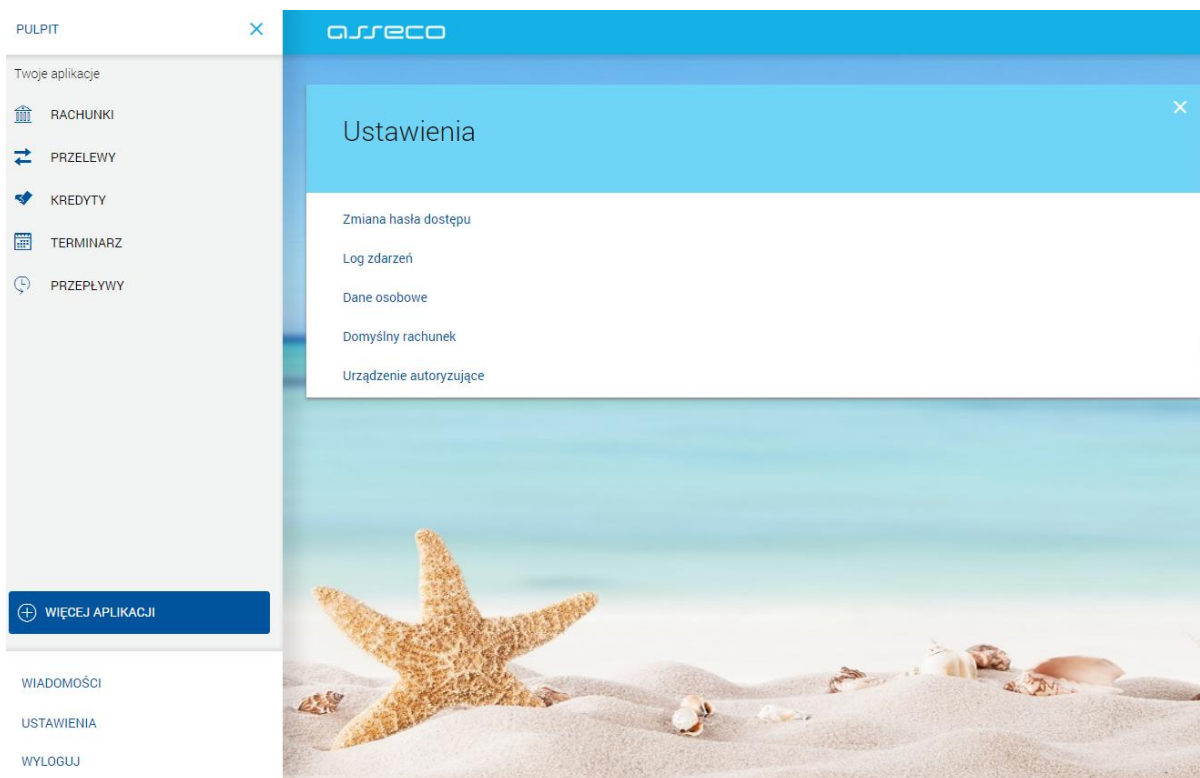


iOS 9.x i now.

UWAGA: ASSECO MAA podczas swojego działania wymaga zapewnienia dostępu do sieci Internet. Po pojawieniu się komunikatu o **aktualizacji aplikacji**, należy zaktualizować ją w sklepie: Google Play lub App Store postępując tak jak przy pobraniu.

Powiązanie urządzenia mobilnego z bankowością elektroniczną

- W bankowości elektronicznej wybieramy zakładkę **USTAWIENIA**, następnie **Urządzenie autoryzujące**.



- Używamy przycisku **POSIADAM APLIKACJĘ**

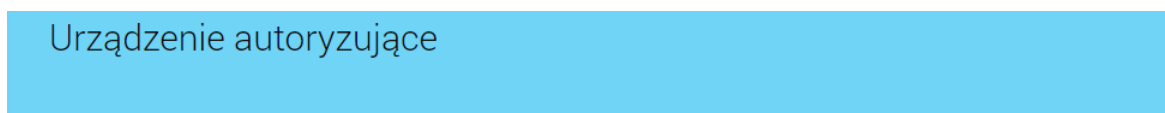


Do autoryzacji urządzenia wymagana jest aplikacja mToken Asseco MAA

Jeśli nie posiadasz aplikacji, znajdziesz ją w Google Play lub App Store

POSIADAM APLIKACJĘ

- Na telefon przychodzi **kodeks SMS**, który należy wprowadzić do bankowości



Wprowadź kod SMS

Kod autoryzacyjny został wysłany za pomocą SMS na numer:

+48 530 *** **2

Wpisz kod

Operacja nr 3 z dnia 26.08.2019

KOD SMS NIE DOTARŁ

POTRZEBUJĘ POMOCY

DALEJ

- Następnie po wyborze przycisku [DALEJ] zostanie wyświetlona formatka z drugim krokiem procesu, na której prezentowany jest kod aktywacyjny.

685 683

Kod aktywacyjny

Wprowadź powyżej wygenerowany kod w aplikacji mToken Asseco MAA

Kod jest ważny przez 5 minut

- Kod aktywacyjny należy wprowadzić w aplikacji mobilnej Asseco MAA podczas rejestracji urządzenia.

W celu zarejestrowania urządzenia autoryzującego, w aplikacji mobilnej Asseco MAA należy wybrać przycisk [ROZPOCZNIJ].

- Pojawi się ekran rejestracji urządzenia, gdzie należy wprowadzić poprawny **kod aktywacyjny** z bankowości



- W kolejnym kroku w celu identyfikacji należy wprowadzić **kod weryfikacyjny** z SMS otrzymany na wskazany nr telefonu.

The screenshot shows the 'Asseco' app interface during the registration process. At the top, there is a header with the 'Asseco' logo and a blue bar containing a back arrow, the text 'REJESTRACJA URZĄDZENIA', and a close 'X' icon. Below the header is a circular icon of a computer monitor. The main text reads: 'W celu identyfikacji konieczne jest podanie kodu weryfikacyjnego, który zostanie przesłany za pomocą SMS'. Below this is a text input field with the placeholder 'Wprowadź kod weryfikacyjny'. Underneath is a numeric keypad with digits 1-9, 0, and a backspace icon. At the bottom is a blue button with a right arrow and the text 'DALEJ'.

- W następnym kroku należy wprowadzić własny **kode PIN**, który będzie służył do logowania do aplikacji Asseco MAA. Nadawany numer PIN musi zawierać od 5 do 8 cyfr i nie może składać się z ciągu takich samych cyfr lub podobnych np. 11111, 222222, 123123, 12345, itp.

The screenshot shows the 'Asseco' app interface during the registration process. At the top, there is a header with the 'Asseco' logo and a blue bar containing a back arrow, the text 'REJESTRACJA URZĄDZENIA', and a close 'X' icon. Below the header is a circular icon of a computer monitor. The main text reads: 'Wprowadź PIN, który będzie służył do logowania do aplikacji'. Below this is a text input field with the placeholder 'Wprowadź PIN' and a question mark icon. Underneath is a numeric keypad with digits 1-9, 0, and a backspace icon. At the bottom is a blue button with a right arrow and the text 'DALEJ'.

- W kolejnym kroku należy ponownie wprowadzić ten sam **PIN** w celu kontroli prawidłowości i zgodności zdefiniowanego kodu PIN.

Po wykonaniu powyższych czynności aplikacja potwierdzi aktywację odpowiednim komunikatem:



- Po poprawnej aktywacji urządzenia użytkownik zostanie przekierowany na ekran główny aplikacji, poprzez który będzie miał możliwość zalogowania się do aplikacji mobilnej za pomocą kodu PIN zdefiniowanego w procesie rejestracji urządzenia autoryzującego.

REALIZACJA PRZELEWU

Po uruchomieniu systemu CUI <https://cbp.cui.pl> wyświetlane jest okno logowanie użytkownika.

- Aby zalogować się do systemu należy w polu Numer Identyfikacyjny wprowadzić identyfikator użytkownika (PC.....) i użyć przycisku [DALEJ].

The screenshot shows a blue header with the word 'LOGOWANIE' on the left and 'PL' with a dropdown arrow on the right. Below the header is a white area with a form. The form has a label 'Numer Identyfikacyjny' followed by a text input field containing the placeholder text 'Wpisz numer'. Below the input field is a blue button labeled 'DALEJ'. Underneath the button is a lock icon and the text 'Pamiętaj o podstawowych zasadach bezpieczeństwa.' followed by a list of instructions: 'Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:' followed by three bullet points: 'o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)', 'o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka', and 'o certyfikat jest wystawiony dla Asseco Poland S.A. przez firmę DigiCert Inc'. Below the list is the text 'Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.' and a link 'Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa'.

- Następnie należy wpisać wybrane znaki z hasła (hasło maskowane) – w polu Kod dostępu, pozostałe znaki z hasła są ukryte i zastąpione znakiem „ • ”. Po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

The screenshot shows a blue header with a back arrow on the left and the word 'LOGOWANIE' on the right. Below the header is a white area with a form. The form has a label 'Kod dostępu' followed by 24 input fields, each containing a black dot. Above the input fields are numbers 1 through 24. Below the input fields is a blue button labeled 'ZALOGUJ'. Underneath the button is a lock icon and the text 'Pamiętaj o podstawowych zasadach bezpieczeństwa.' followed by a list of instructions: 'Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:' followed by three bullet points: 'o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)', 'o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka', and 'o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę Thawte lub DOMENY.PL'. Below the list is the text 'Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem ani też instalacji jakichkolwiek aplikacji na telefonach/komputerach użytkowników.' and a link 'Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa'.

Po wprowadzeniu (w polu Kod dostępu) poprawnego kodu uwierzytelniającego należy użyć przycisku [ZALOGUJ]. System weryfikuje wprowadzone dane i jeżeli stwierdzi ich poprawność, użytkownik zostanie zalogowany.

- Po uruchomieniu systemu bankowości uzupełniamy dane do przelewu
- Klikamy **DALEJ**
- Logujemy się do aplikacji przez wpisanie **PINU**
- Klikam **AKCEPTUJ**
- Potwierdzamy wpisaniem **PINU** i **[ZATWIERDZAMY]**
- Wyświetla się okno operacja zakończona pomyślnie

